What is a DDoS attack?

DDoS attacks are a primary concern in Internet security today. Explore details about how DDoS attacks function, and how they can be stopped.

Learning Objectives

After reading this article you will be able to:

- Define a DDoS attack
- Explain the general structure of a DDoS attack
- Differentiate between the 3 major categories of DDoS attacks
- Understand several DDoS mitigation strategies

RELATED CONTENT

DDoS mitigation
How to DDoS
Denial of service
What is a DDoS botnet?
What is IP spoofing?

Want to keep learning?

Subscribe to theNET, Cloudflare's monthly recap of the Internet's most popular insights!

Subscribe to theNET

Refer to Cloudflare's Privacy Policy to learn how we collect and process your personal data.

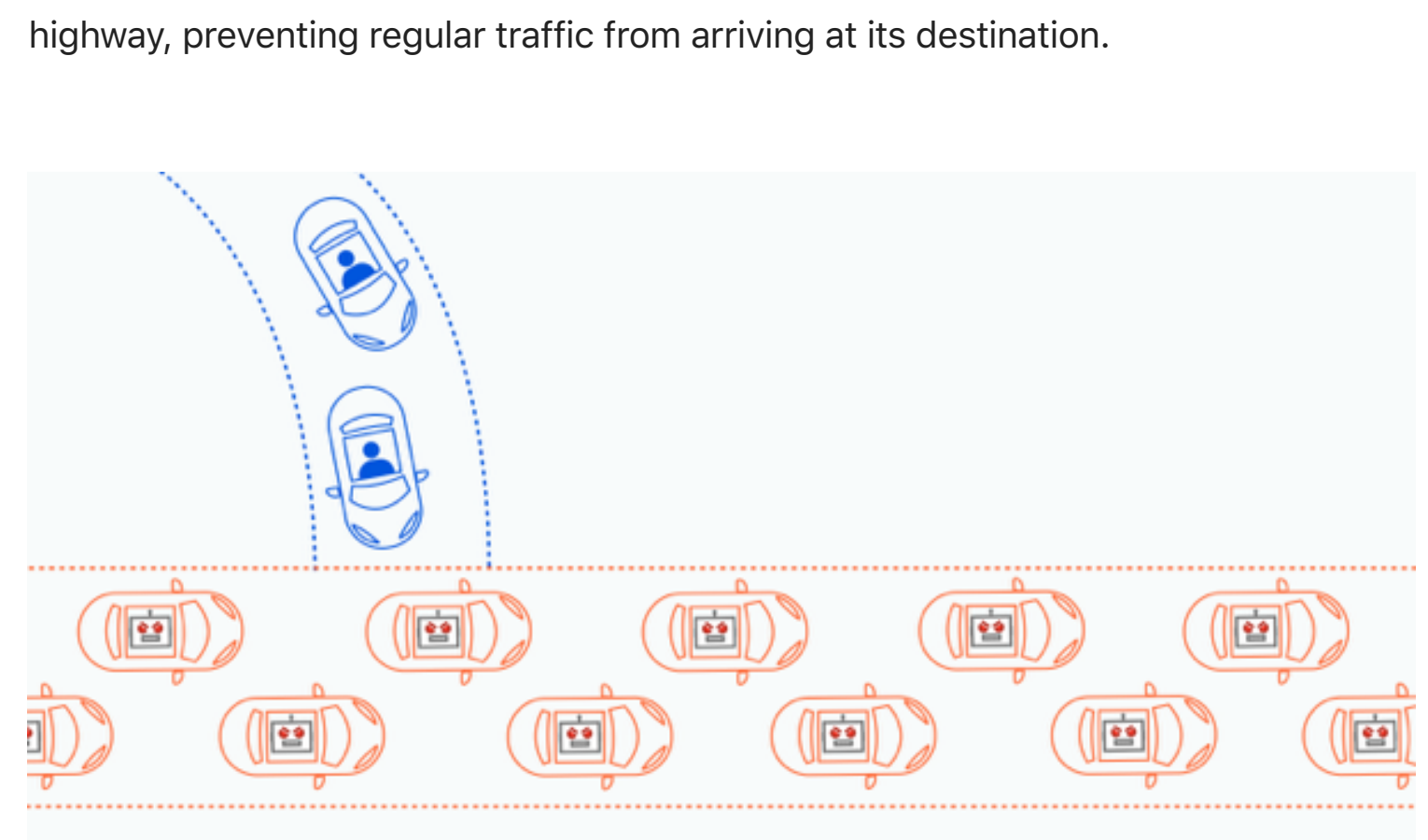
Copy article link

What is a DDoS attack?

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.



Guide
5 things to consider when mitigating DDoS attacks
Get the guide

Talk to an expert
Learn how Cloudflare can protect your business
Contact sales

How does a DDoS attack work?

DDoS attacks are carried out with networks of Internet-connected machines.

These networks consist of computers and other devices (such as IoT devices)which have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots (or zombies), and a group of bots is called a botnet.

Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot.

When a victim's server or network is targeted by the botnet, each bot sends requests to the target's IP address, potentially causing the server or network to become overwhelmed, resulting in a denial-of-service to normal traffic.

Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult.

How to identify a DDoS attack

The most obvious symptom of a DDoS attack is a site or service suddenly becoming slow or unavailable. But since a number of causes — such a legitimate spike in traffic — can create similar performance issues, further investigation is usually required. Traffic analytics tools can help you spot some of these telltale signs of a DDoS attack:

- Suspicious amounts of traffic originating from a single IP address or IP range
- A flood of traffic from users who share a single behavioral profile, such as device type, geolocation, or web browser version
- An unexplained surge in requests to a single page or endpoint
- Odd traffic patterns such as spikes at odd hours of the day or patterns that appear to be unnatural (e.g. a spike every 10 minutes)

There are other, more specific signs of DDoS attack that can vary depending on the type of attack.

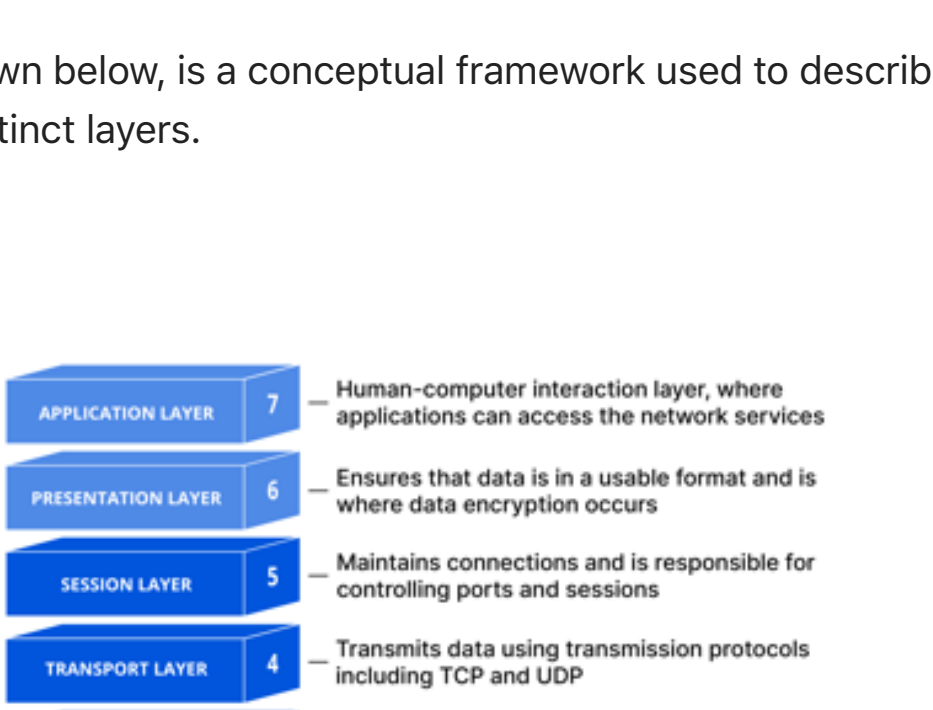
DDoS Protection Get DDoS protection with any Cloudflare plan Get started free

What are some common types of DDoS attacks?

Different types of DDoS attacks target varying components of a network connection. In order to understand how different DDoS attacks work, it is necessary to know how a network connection is made.

A network connection on the Internet is composed of many different components or "layers". Like building a house from the ground up, each layer in the model has a different purpose.

The OSI model, shown below, is a conceptual framework used to describe network connectivity in 7 distinct layers.


APPLICATION LAYER 7 Human-computer interaction layer, where applications can access the network services
PRESENTATION LAYER 6 Ensures that data is in a usable format and is where data encryption occurs
SESSION LAYER 5 Maintains connections and is responsible for controlling ports and sessions
TRANSPORT LAYER 4 Transmits data using transmission protocols including TCP and UDP
NETWORK LAYER 3 Decides which physical path the data will take
DATA LINK LAYER 2 Defines the format of data on the network
PHYSICAL LAYER 1 Transmits raw bit stream over the physical medium

While nearly all DDoS attacks involve overwhelming a target device or network with traffic, attacks can be divided into three categories. An attacker may use one or more different attack vectors, or cycle attack vectors in response to counter measures taken by the target.

Application layer attacks

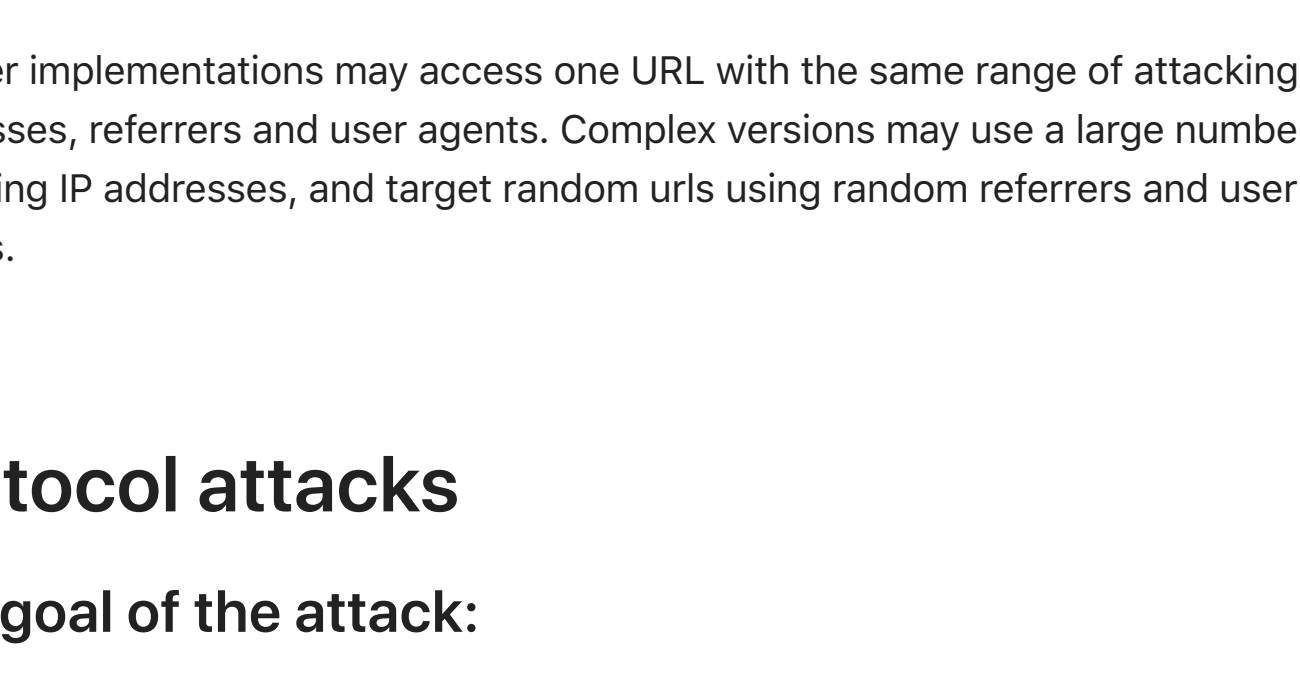
The goal of the attack:

Sometimes referred to as a layer 7 DDoS attack (in reference to the 7th layer of the OSI model), the goal of these attacks is to exhaust the target's resources to create a denial-of-service.

The attacks target the layer where web pages are generated on the server and delivered in response to HTTP requests. A single HTTP request is computationally cheap to execute on the client side, but it can be expensive for the target server to respond to, as the server often loads multiple files and runs database queries in order to create a web page.

Layer 7 attacks are difficult to defend against, since it can be hard to differentiate malicious traffic from legitimate traffic.

Application layer attack example:



HTTP flood

This attack is similar to pressing refresh in a web browser over and over on many different computers at once – large numbers of HTTP requests flood the server, resulting in denial-of-service.

This type of attack ranges from simple to complex.

Simpler implementations may access one URL with the same range of attacking IP addresses, referrers and user agents. Complex versions may use a large number of attacking IP addresses, and target random urls using random referrers and user agents.

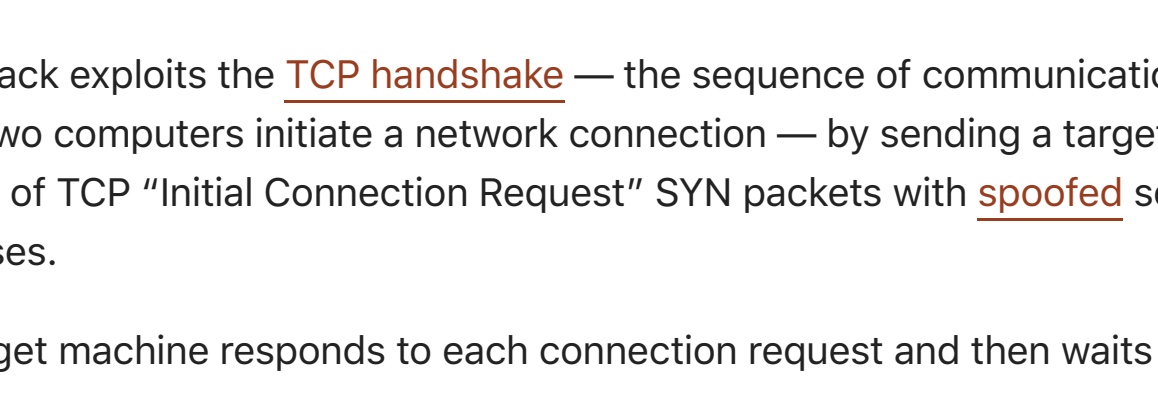
Protocol attacks

The goal of the attack:

Protocol attacks, also known as a state-exhaustion attacks, cause a service disruption by over-consuming server resources and/or the resources of network equipment like firewalls and load balancers.

Protocol attacks utilize weaknesses in layer 3 and layer 4 of the protocol stack to render the target inaccessible.

Protocol attack example:



SYN flood

A SYN Flood is analogous to a worker in a supply room receiving requests from the front of the store.

The worker receives a request, goes and gets the package, and waits for confirmation before bringing the package out front. The worker then gets many more package requests without confirmation until they can't carry any more packages, become overwhelmed, and requests start going unanswered.

This attack exploits the TCP handshake — the sequence of communications by which two computers initiate a network connection — by sending a target a large number of TCP "Initial Connection Request" SYN packets with spoofed source IP addresses.

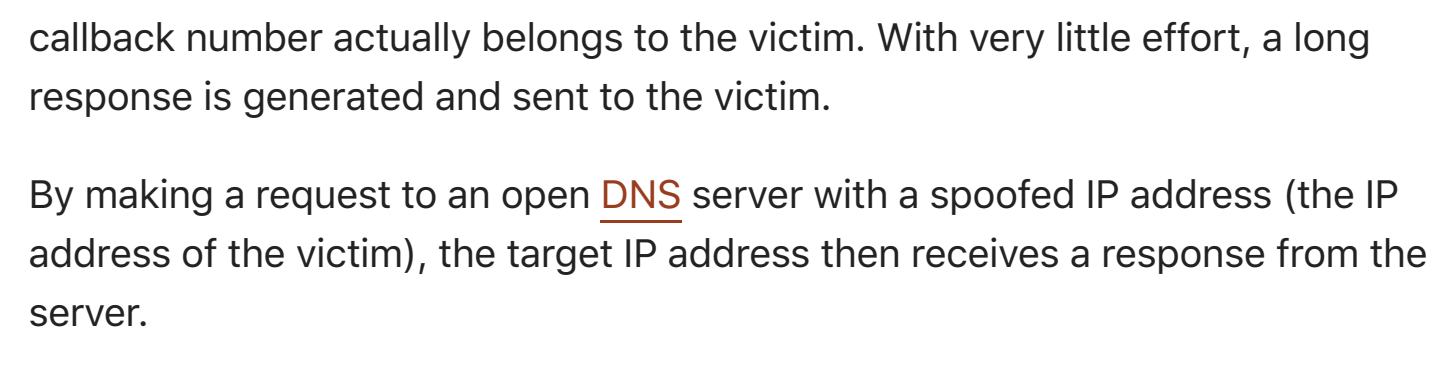
The target machine responds to each connection request and then waits for the final step in the handshake, which never occurs, exhausting the target's resources in the process.

Volumetric attacks

The goal of the attack:

This category of attacks attempts to create congestion by consuming all available bandwidth between the target and the larger Internet. Large amounts of data are sent to a target by using a form of amplification or another means of creating massive traffic, such as requests from a botnet.

Amplification example:



DNS Amplification

A DNS amplification is like if someone were to call a restaurant and say "I'll have one of everything, please call me back and repeat my whole order," where the callback number actually belongs to the victim. With very little effort, a long response is generated and sent to the victim.

By making a request to an open DNS server with a spoofed IP address (the IP address of the victim), the target IP address then receives a response from the server.

What is the process for mitigating a DDoS attack?

The key concern in mitigating a DDoS attack is differentiating between attack traffic and normal traffic.

For example, if a product release has a company's website swamped with eager customers, cutting off all traffic is a mistake. If that company suddenly has a surge in traffic from known attackers, efforts to alleviate an attack are probably necessary.

The difficulty lies in telling the real customers apart from the attack traffic.

In the modern Internet, DDoS traffic comes in many forms. The traffic can vary in design from un-spoofed single source attacks to complex and adaptive multi-vector attacks.

A multi-vector DDoS attack uses multiple attack pathways in order to overwhelm a target in different ways, potentially distracting mitigation efforts on any one trajectory.

An attack that targets multiple layers of the protocol stack at the same time, such as a DNS amplification (targeting layers 3/4) coupled with an HTTP flood (targeting layer 7) is an example of multi-vector DDoS.

Mitigating a multi-vector DDoS attack requires a variety of strategies in order to counter different trajectories.

Generally speaking, the more complex the attack, the more likely it is that the attack traffic will be difficult to separate from normal traffic - the goal of the attacker is to blend in as much as possible, making mitigation efforts as inefficient as possible.

Mitigation attempts that involve dropping or limiting traffic indiscriminately may throw good traffic out with the bad, and the attack may also modify and adapt to circumvent countermeasures. In order to overcome a complex attempt at disruption, a layered solution will give the greatest benefit.

Blackhole routing

One solution available to virtually all network admins is to create a blackhole route and funnel traffic into that route. In its simplest form, when blackhole filtering is implemented without specific restriction criteria, both legitimate and malicious network traffic is routed to a null route, or blackhole, and dropped from the network.

If an Internet property is experiencing a DDoS attack, the property's Internet service provider (ISP) may send all the site's traffic into a blackhole as a defense. This is not an ideal solution, as it effectively gives the attacker their desired goal: it makes the network inaccessible.

Rate limiting

Limiting the number of requests a server will accept over a certain time window is also a way of mitigating denial-of-service attacks.

While rate limiting is useful in slowing web scrapers from stealing content and for mitigating brute force login attempts, it alone will likely be insufficient to handle a complex DDoS attack effectively.

Nevertheless, rate limiting is a useful component in an effective DDoS mitigation strategy. Learn about Cloudflare's rate limiting

Web application firewall

A Web Application Firewall (WAF) is a tool that can assist in mitigating a layer 7 DDoS attack. By putting a WAF between the Internet and an origin server, the WAF may act as a reverse proxy, protecting the targeted server from certain types of malicious traffic.

By filtering requests based on a series of rules used to identify DDoS tools, layer 7 attacks can be impeded. One key value of an effective WAF is the ability to quickly implement custom rules in response to an attack. Learn about Cloudflare's WAF.

Anycast network diffusion

This mitigation approach uses an Anycast network to scatter the attack traffic across a network of distributed servers to the point where the traffic is absorbed by the network.

Like channeling a rushing river down separate smaller channels, this approach spreads the impact of the distributed attack traffic to the point where it becomes manageable, diffusing any disruptive capability.

The reliability of an Anycast network to mitigate a DDoS attack is dependent on the size of the attack and the size and efficiency of the network. An important part of the DDoS mitigation implemented by Cloudflare is the use of an Anycast distributed network.

Cloudflare has a 280 Tbps network, which is an order of magnitude greater than the largest DDoS attack recorded.

If you are currently under attack, there are steps you can take to get out from under the pressure. If you are on Cloudflare already, you can follow these steps to mitigate your attack.

The DDoS protection that we implement at Cloudflare is multifaceted in order to mitigate the many possible attack vectors. Learn more about Cloudflare's DDoS protection and how it works.

Getting Started
Free plans
For enterprises
Compare plans
Get a recommendation
Request a demo
Contact sales

About DDoS attacks
What is a DDoS attack?
What is a DDoS botnet?
Famous DDoS attacks
DDoS mitigation

DDoS attacks
ACK flood attack
Application layer attack
Cryptocurrency attacks
DNS amplification attack
DNS flood attack
HTTP flood attack
Layer 3 attacks
Low and slow attack
Memcached DDoS attack
NTP amplification attack
Ping (ICMP) flood attack
QUIC flood attack
Ransom DDoS attack
SSDP attack
SYN flood attack
UDP flood attack
Ping of death (historic)
Smurf attack (historic)

DDoS attack tools
How to DDoS
DDoS booter/IP stresser
High Orbit Ion Cannon
Low Orbit Ion Cannon
IP spoofing
Malware
Mirai botnet
R U Dead Yet? (R.U.D.Y.)
Slowloris attack

DDoS glossary
What is Anonymous Sudan?
Blackhole routing
Denial of service
HTTP
ICMP
Internet of Things (IoT)
Layer 7
OSI Model
TCP/IP
User Datagram Protocol (UDP)
Web application firewall (WAF)
How to prevent DDoS attacks

Learning Center navigation
Learning Center Home
DNS Learning Center
CDN Learning Center
Serverless Learning Center
Security Learning Center
Performance Learning Center
SSL Learning Center
Bots Learning Center
Cloud Learning Center
Access Management Learning Center
Network Layer Learning Center
Privacy Learning Center
Video Streaming Learning Center
Email Security Learning Center
AI Learning Center

© 2024 Cloudflare, Inc. | Privacy Policy | Terms of Use | Report Security Issues | ✓✕ Cookie Preferences | Trademark